Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1615 04/11/14

~ The History of Atari! ~ People Are Talking! ~ Sony’s Yoshida on PS!
~ GOP Granted .gop Domain ~ Google Glass 1-Day Sale ~ AT&T Hacker Is Freed!
~ Heartbleed, Understand! ~ Super Smash Brothers! ~ Date Set for ET Dig!

~ Feds Address Concerns! ~ IBM Mainframe Turns 50! ~ Facebook Censorship!

-* A Race To Plug Internet Hole *-
-* NSA Denies It Exploited Heartbleed! *-
-* New Heartbleed Bug Poses Major Data Threat *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""

Another crazy week - what else is new! However, I did want to make mention of a couple of things this week, at least briefly. If using an Atari system is only a "part-time" use; and you use a PC for some or most of your computing needs, you may still be using Windows XP (like me). If so, you are likely aware that Microsoft has ended its support of the XP operating system. That means that new future threats such as hacking, etc. will no longer be "protected". This week, we offer a few articles pertaining to this predicament. Personally, I will continue to use my XP machine, but I will phase out its use; I recently purchased my first Mac computer. Once I get used to it and ported over most of my applications, my PC use will be restricted to certain functions that I may not be able to easily do on the Mac (at least for the present time). It's time, and I've had enough of the Windows environment!

The other piece of news unveiled this week is the "Heartbleed" bug which poses a major threat to user data. Hopefully, although the total impact of this threat has not been identified yet, is that web sites and related servers fix these holes quickly. As depicted in the numerous articles in this week's issue, the repairs have begun, Do what you can to further protect yourself!

Until next time...

=~=~=~=

->In This Week's Gaming Section - New Super Smash Brotherss Out This Summer!
"""""""""""""""""""""""""""""""" Sony s Yoshida on Two Decades of PlayStation!

IGN Presents: the History of Atari!
And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

"""""""""""""""""""""""""""""""""""""

Nintendo Announces the New Super Smash Brotherss Will Be Out This Summer

Nintendo announced on Tuesday night that the highly anticipated next-gen installment of Super Smash Bros. will finally release on the 3DS this summer and on the Wii U in fall. Along with the release window, Nintendo also went into detail about the visual enhancements of the multiplatform title, the game s dedication to the competitive fighting community and the introduction of some new (and not-so-new) faces.

Unlike previous games in the series, Super Smash Bros. for 3DS and Wii U will run at 60 frames per second, although some of the additional in-game features, such as Pokemon and Assist Trophies, will run at 30 fps.

Both versions of the game will also feature two separate modes of play: For Fun and For Glory. In For Fun mode, players will be thrown into a random stage with all the game s items turned on. In this mode, only wins will be recorded to your profile. If you decide to play For Glory instead, you ll play on an anti-frill Final Destination version of a map, which is completely flat so as not to distract from the battle. In For Glory, your wins and losses will be recorded.

As for new characters, Nintendo revealed that character transformations will no longer be a part of the game, thus allowing Zero Suit Samus, Sheik and Charizard to serve as singular characters this time around. Greninja, a brand new Pokemon, will also be joining the fight, along with the returning egg-tosser, Yoshi.

Sony s Shuhei Yoshida Reflects on Two Decades of PlayStation

With the PlayStation 4, Sony has put forth a narrative of learning from past mistakes and re-focusing on features for the players. At the Computer History Museum in Mountain View, Calif., last night, Sony Worldwide Studios President Shuhei Shu Yoshida traced his own arc through four console generations and talked a bit about what s ahead.

Interviewed by longtime collaborator and PS4 lead system architect Mark Cerny for the museum s Revolutionaries speaker series, Yoshida said his role has changed greatly over the years. Shu 1.0 was a business development guy, the first to join the team of 20-odd engineers developing the PlayStation under Ken Kutaragi, in 1993.

 At the time, consoles were considered a kids toy, Yoshida said.
 Someone in management said we should not go into the toy business, so we named it Sony Computer Entertainment.

At first, he was only working with Japanese game publishers like Namco, Konami and Square Enix, but Yoshida recounted how Cerny showed up in Japan, insistent on obtaining a PlayStation development kit for his company at the time, the Silicon Valley-based Crystal Dynamics. The hitch was that Sony had only Japanese versions of the development contracts, but Cerny came back and signed for the kit all the same.

As Yoshida later found out, Cerny didn t have the signing power with Crystal Dynamics to broker such a major deal.

The two worked together on the first Crash Bandicoot game alongside future Sony Computer Entertainment president and CEO Andrew House, the game s marketing VP. Shu 2.0? focused more and more on America and less on Japan, losing interest in the legacy developers from his home country. Even though he has since moved back to Japan, Yoshida maintained that it s still tough for Japanese publishers in the console world.

 They should really focus on what they do best, he said. Many games try to appease Western audiences, not understanding the culture, and most of them fail.

 Shu 3.0, the current model, oversees all game production in the PlayStation world. However, Yoshida has increasingly become part of the console s public face, appearing in a viral video mocking Microsoft s initially announced (now abandoned) restrictions on sharing video game discs on Xbox One:

He described himself as unofficial customer service because his morning routine includes using his tablet to check Twitter for gamers with complaints or feature suggestions. Twitter is more and more becoming part of my job, he added, with both Sony and outside game developers asking him to tweet things on behalf of their products and games.

Yoshida doesn t only tweet about PlayStation games, though. He owns two units of all the gaming consoles since some titles on some systems are region-locked to Japan, and has been banned twice, but seemingly temporarily from Nintendo s Wii social community, Miiverse. First, he tried to use his Twitter handle @yosp as his Miiverse name, but was told that was against the rules. He now goes by ShuYoshida, but was reprimanded a second time when he posted I <3 PS," referring to PlayStation.

 You re not supposed to promote a commercial product in Miiverse, Yoshida said.

But what s next for PlayStation now that the PS4 is out and selling well? In a brief interview with Re/code after the Revolutionaries interview, Yoshida said he s happy with Facebook s acquisition of Oculus VR because it validates Sony s own nascent virtual reality headset, Project Morpheus. Now, he said, it s Sony vs. Facebook rather than Sony vs. a startup.

He also indicated that as the cloud gaming service PlayStation Now test-launches this summer, Sony will shift to [be] service-oriented, delivering games to new devices that couldn t previously play them. All of which raises the question: In six or seven years, will there be a need for a PlayStation 5?

 It s really up to the game creators, Yoshida said. If they still feel that we need more machine power We want to realize this and that and that, but we cannot do [it] with PS4' if that s the case, there s a good reason to have PS5, so that developers can create their vision. So, we ll see.

=~=~=~=

IGN Presents: the History of Atari

(Part 3 of 4)

In 1976, Bushnell - having bought out his co-founder, Ted Dabney, in 73 - sold Atari to entertainment conglomerate Warner Communications for a widely-publicized $28 million (of which Bushnell personally received in the region of $15 million). This, it would turn out, was the beginning of Atari s first death, and it wouldn t be all that long before Bushnell s involvement with the company he created would come to an end. Before that happened, though, there was another massively important Atari invention to come: the VCS, the home games console later known as the Atari 2600.

This was the beginning of Atari s first death.

I was born in 1988. When I was growing up, I had games consoles, Cartoon Network, movies on tape - kids entertainment had become, by that point, totally commercialized and massively over-served. But in the Seventies, in the UK, there existed three TV channels, and programming for kids left a lot to be desired. During the summer of 1979, an 11-week ITV strike added insult to injury. My older friends tell me that kids had to actually go outside - or read comics, play records or fiddle with Lego. Sure, video games existed in the latter half of the 70s, but only in the most primitive sense imaginable; if you wanted to play games outside of your local arcade, you most likely had a cheap knock-off Pong system, or some handheld abomination. Honestly, childhood in the seventies sounds exceptionally boring. Just as well the music was so good.

It s not hard to see why the first home computers, and the games that came with them, had such a gigantic impact on that generation.

The story of the Atari VCS (later rebranded the Atari 2600) technically starts in 1975, when Atari was looking for a way to bring all of its successful arcade games to the home (the project was codenamed Stella). What made it happen was the release of the MOS Technology 6052, the first affordable microprocessor, which was one of the technological revolutions that made home computers possible. The Atari VCS would use it, as would its cousins the Atari 400 and 800 home computer, the Apple II, the NES, the BBC Micro and the Commodore 64. Combined with the ROM cartridge, an extremely cheap way of storing the games themselves, it represented a way to get quality video games into the home without asking people to pay thousands of dollars.

But Atari couldn t afford to produce it, even though Bushnell suspected that it could be a huge hit. Meanwhile, other companies were making forays into cartridge-based home gaming, further eroding the sales of Atari s home Pong units. This need for cash is what motivated the sale to Warner - the company promised to finance the manufacturing of the VCS as quickly as possible following the acquisition.

Released in October 1977 in the US, and the following year in Europe, the

Atari VCS shipped with two joysticks that have since become icons of video games, and was also compatible with a keypad and paddle controllers. It cost $199 - the equivalent of nearly $800 today. It would eventually be one of the most successful games consoles ever, but bizarrely, it would take years to get up to speed. The pricing, combined with the public s slow realization that you could play something other than Pong on the VCS (and everybody had had quite enough of Pong by 1977), held it back. It underperformed in both 1977 and 1978, selling only just over half its manufactured stock. By the end of 1978 only around 750,000 machines had been sold, despite a $5,000,000 marketing spend by Warner.

It was in 1978 that Nolan Bushnell left the company. His Atari was always known for its legendarily laid-back, creative working environment. Bushnell literally hosted hot-tub parties, and company retreats were famous for the prevalence of drink and drugs. Megacorp Warner could hardly have been a more different prospect, and higher-ups hated Bushnell and his engineers Friday parties and lax dress code. Following repeated disagreements with the company s new owners and managers, including a stand-up row with a Warner executive in front of the board, Bushnell got himself fired. His entrepreneurial spirit would see him involved in a huge array of other companies - but in interviews, you always sense that he would have loved to have taken Atari forwards himself.

In 1979, though, under new CEO Ray Kassar, everything would change. Taito s Space Invaders had hit the arcades and caused an explosion of interest in games again, and Warner continued to spend more marketing money on the VCS. It became a best-seller, selling a million units in 1979 alone. It was the home conversion of Space Invaders that really did big business - in 1980 the Atari 2600 sold two million units. The console continued selling double what it had the year before, until it hit 10 million in annual sales in 1982. Having started out as almost a flop, the Atari VCS had become dominant. Meanwhile, the architecture was adapted for the Atari 400 and 800 home computers, which became widely available in 1979 and had both a cartridge slot and a keyboard.

The idea of being able to play arcade games at home was mind-blowing at the time. But the VCS didn t just offer the games people already knew in a home setting - there were hundreds of games coming out for it, from Atari s own (Adventure, Yar s Revenge) to third-party games from opportunistic software houses. It proved to be a fertile development ecosystem.

In 1982 Atari s revenues made up a stunning 70% of its parent company Warner s income - bigger than music, bigger than film. But even as the Atari 2600 became a huge worldwide hit, new CEO Ray Kassar had been gutting the parts of the company that would have been able to follow it up. The R&D department was cut in 1979, replaced largely with more marketing staff, with the aim of to dissolving the influence that Atari s creative engineers had enjoyed under Bushnell. These changed caused the people actually making games at Atari to leave in droves from 1979 onwards, massively frustrated by management and the lack of credit they were getting for their creations.

In 1979, four of Atari s best former engineers started a new company called Activision. Their aim: to make games for the VCS that were better and would sell better than Atari s own. This would be the beginning of third-party publishing. Warner could not abide this. With both the Atari 400/800 series of home computers and the games-centric VCS, Warner wanted to own everything: hardware, software, the lot. Instead of making open

platforms for developers to play with, they wanted a closed system. In 1981, Atari actually sued Activision for making games for its console. Activision s games were massively successful on the VCS and Atari continued to hit them with lawsuits, to no effect. The modern equivalent of this legal battle would be Microsoft suing EA for selling so many copies of FIFA on Xbox - the video game industry has come a long ways since 1981.

Meanwhile, there was a huge glut of low-quality software jamming up the market - much of it coming from within Atari itself, including a lackluster Pac-Man conversion in 1982. The so-called video game crash of 1983 would hit Atari extremely hard. Unsold merchandise was dumped in the desert and covered with concrete (according to a New York Times report from August 1983), reportedly including thousands of copies of the famously atrocious E.T. The Videogame. A Microsoft-funded documentary is hoping to excavate the site this year. Atari lost an astonishing $310.5 million in the second quarter of 1983 alone.

Date Set for New Mexico Dig for Atari ’E.T.’ Games

Organizers of a search in a New Mexico landfill for a rumored stash of what some call the worst video game ever made by Atari announced Thursday that the dig will get underway this month.

The dig at the Alamogordo landfill where Atari reportedly discarded millions of "E.T. the Extra-Terrestrial" game cartridges in 1983 is scheduled for April 26, officials with Microsoft-owned Xbox said.

The excavation will be open for public viewing, according to Xbox.

The company is joining with Fuel Entertainment and LightBox Interactive to search the landfill. All three companies are making a documentary about the project. Microsoft plans to release the documentary on its Xbox One console.

City officials told the Alamogordo Daily News on Wednesday that the city has rights to any discovered games. City Attorney Stephen Thies said any game cartridges will be stored by the city for possible marketing. However, a tentative agreement between the Alamogordo City Commission and Fuel Entertainment’s parent company calls for Fuel to receive some games.

The city will give Fuel either 100 game cartridges or 10 percent, depending on which is the lesser amount, according to Thies. But Fuel cannot receive more than $2,500 worth of games. The company plans to hand out the cartridges to film crews.

City commissioners also want Fuel’s $1.5 million liability insurance to be raised to $3 million.

"If they decide they don’t want any of the games, then the original $1.5 million insurance will apply." Thies said. "Because it is our landfill, anything that’s out there is our property, if any games are found those are our games."

All three companies gained approval last month from the New Mexico Environmental Department for their waste excavation plan. The agency plans to send a representative to monitor the project once it commences.

Atari paid director Steven Spielberg tens of millions of dollars to license the wildly popular 1982 movie’s name, and game developers completed the project in just six weeks. In the game, the player takes on the role of the titular alien and tries to elude FBI agents while collecting pieces of a telephone to call E.T.’s spaceship.

The end result was a huge commercial dud that caused the troubled company’s worth to sink even further.

Atari purportedly disposed of millions of game cartridges and other equipment by the truckload at the landfill. The area’s supposed role as a gaming burial ground has taken on urban-legend status over the years.

The landfill was first used as a dumping ground in the 1920s but has been closed since the late 1980s, officials said.

Huge Collection Of Classic Games Needs A New Home

Facing mounting financial pressure, the Danish museum Spilmuseet ("The Games Museum") is about to jettison a massive collection of classic video games and related hardware. And with nobody opening their doors yet, all these refugees of console wars past are still in need of a new home.

The collection consists of roughly "10,000 console and computer games, 4,000 arcade games and 1,400 arcade machines," according to the Wall Street Journal. Rune Keller, the museum’s head, told the paper that he’s "pretty sure our arcade collection is the world’s largest." That’s all the more impressive considering that he assembled the whole thing with his dad. The Journal didn’t say how long it took the father-son duo to fill out the collection, but Keller said that they poured "roughly a million dollars" into the project and "invested their spare time in restoring the items."

There are some real gems in the collection, such as a working version of the 1981 arcade game Space Fortress and a European version of the 1979 game Sheriff, the first Nintendo title to feature artwork by Super Mario and The Legend of Zelda creator Shigeru Miyamoto. That’s in addition to classics like Pong and formative consoles from Amiga and Atari.

With so much great stuff at his fingertips, you might be wondering: why is Keller letting it all go? He told the Journal that he decided to hand off the collection after he failed to win over government support for the endeavor. But seeing as he and his dad were able to spend a cool million on this passion project in the first place, Keller isn’t in dire enough financial straits to just let anybody take his games away. Rather, he’s looking for someone (or something) that will purchase the entire collection and keep it in the public eye.

"We think it is important to conserve the history of gaming, just as it is to conserve films, books or music," Keller said. So rather than hand the collection to another individual benefactor or eager gamer, he wants to find a like-minded institution that will use the archive to "serve the public good."

New York City’s Museum of Modern Art ranks as one of the most prestigious museums in the world. You can go there to see iconic creations like

Keller told the Journal that he’s been approached by "organizations from Sweden and France as well as a ’big, established museum in the U.S.’" Several prominent U.S. museums have taken an increased interest in games in recent years, so there’s no telling where the games might find themselves if they end up making the journey across the pond. In any case, it’s nice to see that video games are finally beginning to emerge from their position as "second-class citizens" in the "pantheon of pop culture," as Kill Screen founder Jamin Warren put it back in 2012 when the Museum of Modern Art first introduced them to its permanent collection.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

New Heartbleed Bug Poses Major Threat to Data

A newly discovered bug in widely used web encryption technology has made data on many of the world s major websites vulnerable to theft by hackers in what experts say is one of the most serious security flaws uncovered in recent years.

The finding of the so-called Heartbleed vulnerability, by researchers with Google and the small security firm Codenomicon, prompted the U.S. government s Department of Homeland Security to advise businesses on Tuesday to review their servers to see if they were using vulnerable versions of a type of software known as OpenSSL.

It said updates are already available to address the vulnerability in OpenSSL, which could enable remote attackers to access sensitive data including passwords and secret keys that can decode traffic as it travels across the Internet.

We have tested some of our own services from [an] attacker s perspective. We attacked ourselves from outside, without leaving a trace, Codenomicon said on a website it built to provide information about the threat, heartbleed.com.

Computer security experts warned that means victims cannot tell if their data has been accessed, which is troubling because the bug has existed for about two years.

If a website is vulnerable, I could see things like your password, banking information and healthcare data, which you were under the impression you were sending securely to your website, said Michael Coates, director of product security for Shape Security.

Chris Eng, vice president of research with software security firm Veracode, said he estimates that hundreds of thousands of web and email servers around the globe need to be patched as soon as possible to

protect them from attack by hackers who will rush to exploit the vulnerability now that it is publicly known.

The technology website Ars Technica reported that security researcher Mark Loman was able to extract data from Yahoo Mail servers by using a free tool.

A spokeswoman for Yahoo confirmed that Yahoo Mail was vulnerable to attack but said it had been patched, along with other main Yahoo sites such as Yahoo Search, Finance, Sports, Flickr, and Tumblr.

We are working to implement the fix across the rest of our sites right now, she said Tuesday evening.

After Heartbleed Bug, A Race to Plug Internet Hole

Popular websites and millions of Internet users scrambled to update software and change passwords Wednesday, after a security bug in crucial encryption code was disclosed sooner than researchers had planned.

Facebook Inc. and Yahoo Inc. s blogging site Tumblr advised users to change their passwords because of the so-called Heartbleed bug. Canada s tax agency shut its filing website as a precaution, weeks before its April 30 filing deadline.

Websites for Airbnb Inc., the Four Seasons hotel chain and Netflix Inc. were vulnerable for a time, said Wayne Jackson, CEO of Sonatype Inc., which manages open-source software. Airbnb and Netflix said they had updated their software. Four Seasons didn t immediately respond to a request for comment.

It s easily the worst vulnerability since mass-adoption of the Internet, said Matthew Prince, CEO of CloudFlare Inc., a San Francisco cybersecurity company. It s going to be really bad.

The hole in the Internet was supposed to be fixed quietly. Researchers at Google Inc. who found the bug told the team in charge of the code, OpenSSL Project, last week, said Mark Cox, an OpenSSL manager.

OpenSSL then planned to tell trusted website operators how to fix the bug before making it public Wednesday. Some big sites, including Facebook and Akamai Technologies Inc., did get a heads up, people familiar with the research said.

But managers feared that news of the security hole had leaked to hackers, and so they disclosed it on Monday. That caught companies from Amazon.com Inc. to Yahoo unprepared.

A Yahoo spokeswoman said the company had made the appropriate corrections. Amazon Web Services posted a security bulletin detailing what services it had updated.

The episode illustrates the delicate task of managing the Internet s plumbing to keep it safe for banks, social networks and retailers. When companies find flaws, they have to decide how to tell as many people as possible without tipping off hackers.

If the news gets out too quickly, the patches to fix the bug may not be ready, said Christopher Soghoian, a technologist at the American Civil Liberties Union. Move too slowly, and hackers will learn of the weakness.

A Google spokeswoman declined to comment on who was notified early. Codenomicon, whose researchers also helped find the bug, didn t respond to a request for comment.

The Heartbleed bug is problematic because it affected about two-thirds of Internet servers when it was disclosed Monday. Websites where users have to log in increasingly use encryption to make sure users personal information is unreadable as it traverses the Internet.

The majority, including Internet companies, banks and the federal government, use a free version of this code from OpenSSL, a library of encryption code for websites managed by Mr. Cox and three other European developers.

The bug affected OpenSSL versions released in the past two years. In vulnerable systems, hackers can grab previously encrypted data from a website s server before it is deleted.

Researchers said it is impossible for a website to detect whether or not hackers use the bug to steal data. That means companies can t notify consumers who may have been hacked.

CloudFlare s Mr. Prince said its systems were vulnerable for a time. The company was notified of the bug last week and made the recommended fix after signing a non-dsclosure agreement.

Security teams at Facebook and Akamai, which helps move videos across the Internet, received similar warnings, people familiar with the matter said.

 We added protections for Facebook s implementation of OpenSSL before this issue was publicly disclosed, said a Facebook spokesman, who declined to elaborate. An Akamai spokesman said the company was contacted by the OpenSSL team in advance.

Google also had patched its systems ahead of time. The search giant told users Wednesday they didn t need to change Google passwords.

The Canada Revenue Agency said that, after learning late Tuesday about the Heartbleed bug, it decided to halt access to its online tools that allow individuals and businesses to make tax filings electronically.

In an update Wednesday, the agency said it was working on a remedy to restore online tax-filing services and expected the services to resume sometime this weekend.

Despite being used by most websites, OpenSSL is a relatively overlooked piece of computer code. Many of its contributions come from volunteers, and a team of four core members manage what winds up in the encryption tools used by hundreds of thousands of websites.

After Google contacted it last week, Mr. Cox and his team planned to get patches ready as they notified major Web companies before April 9. They notified some server operating system vendors, including Red Hat Inc. and Canonical Ltd.

On Monday, though, Mr. Cox s team began to worry the bug had leaked after

it received a warning about the bug from the National Cyber Security Centre Finland.

This spooked the group, which decided to disclose the bug Monday. At least one person worked through the night, said Steve Marquess, president of the OpenSSL Software Foundation, which provides funding for the OpenSSL team.

Matthew Green, an encryption expert at Johns Hopkins University, said OpenSSL Project is relatively neglected, given how critical of a role it plays in the Internet. Last year, the foundation took in less than $1 million from donations and consulting contracts.

Donations have picked up since Monday, Mr. Marquess said. This week, it had raised $841.70 as of Wednesday afternoon.

What You Need To Know About The Heartbleed Bug

Millions of passwords, credit card numbers and other personal information may be at risk as a result of a major breakdown in Internet security revealed earlier this week.

The damage caused by the "Heartbleed" bug is currently unknown. The security hole exists on a vast number of the Internet’s Web servers and went undetected for more than two years. While it’s conceivable that the flaw was never discovered by hackers, it’s nearly impossible to tell.

There isn’t much that people can do to protect themselves until the affected websites implement a fix.

Here are answers to some common questions about Heartbleed and how you can protect yourself:

Q: What is Heartbleed and why is it a big deal?

A: Heartbleed affects the encryption technology designed to protect online accounts for email, instant messaging and e-commerce. It was discovered by a team of researchers from the Finnish security firm Codenomicon, along with a Google Inc. researcher who was working separately.

It’s unclear whether any information has been stolen as a result of Heartbleed, but security experts are particularly worried about the bug because it went undetected for more than two years.

Q: How does it work?

A: Heartbleed creates an opening in SSL/TLS, an encryption technology marked by the small, closed padlock and "https:" on Web browsers to show that traffic is secure. The flaw makes it possible to snoop on Internet traffic even if the padlock is closed. Interlopers can also grab the keys for deciphering encrypted data without the website owners knowing the theft occurred.

The problem affects only the variant of SSL/TLS known as OpenSSL, but that happens to be one of the most common on the Internet.

Q: So if the problem has been identified, it’s been fixed and I have nothing to worry about. Right?

A: It depends on the website. A fixed version of OpenSSL has been released, but it’s up to the individual website administrators to put it into place.

Yahoo Inc., which has more than 800 million users around the world, said Tuesday that most of its popular services including sports, finance and Tumblr had been fixed, but work was still being done on other products that it didn’t identify.

Q: So what can I do to protect myself?

A: Ultimately, you’ll need to change your passwords, but that won’t do any good until the sites you use adopt the fix. It’s also up to the Internet services affected by the bug to let users know of the potential risks and encourage them to change their passwords.

Q: I plan to file my income taxes online. Is that safe considering how much personal information is involved?

A: The IRS released a statement on Wednesday saying that it’s not affected by the bug or aware of any related security flaws. It advised taxpayers to continue filing their returns as they normally would in advance of the April 15 deadline.

But Canada’s tax agency on Wednesday temporarily cut off public access to its electronic filling services just three weeks before its tax deadline citing Heartbleed-related security concerns.

The Canada Revenue Agency said it’s working to restore secure access as soon as possible. The agency said consideration will be given to taxpayers who are unable to comply with their filing requirements because of the interruption.

NSA Denies Report It Exploited Heartbleed for Years

The Heartbleed security flaw that exposes a vulnerability in encryption has reportedly extended its reach well beyond Web services.

According to Bloomberg, citing "two people familiar with the matter," the National Security Agency knew about Heartbleed for at least two years and used the hole in encryption technology to gather intelligence.

However, the agency strongly denied the substance of Bloomberg’s report.

"NSA was not aware of the recently identified vulnerability in OpenSSL, the so-called Heartbleed vulnerability, until it was made public in a private-sector cybersecurity report,’’ the agency said in a statement. "Reports that say otherwise are wrong."

This follows a separate Bloomberg report the security flaw impacts Android smartphones and tablets that run the 4.1.1 version of the Google operating system.

In a statement on Google’s online security blog, the company says patching information has been submitted to partners.

Meanwhile, The Wall Street Journal reports some network products created by Cisco and Juniper contain the flaw. The vulnerability affects products such as routers and firewalls.

In an update published Thursday, Cisco says multiple products incorporate OpenSSL, a variation of the Secure Sockets Layer (SSL) protocol used to encrypt sensitive data.

A spokesperson for Juniper tells the Journal updating equipment to patch up the security hole could take some time.

Heartbleed is a flaw that would allow anyone to read the memory of servers running OpenSSL, which leaves information such as usernames, passwords and credit card data exposed.

"This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users," says Codenomicon, a security firm that helped uncover Heartbleed and established a website to inform others.

Web services have scrambled since the revelation of Heartbleed to fix the bug. Several companies including Facebook, Google and Yahoo have confirmed they are clear. Most recently, Apple confirmed to Re/code its services like iOS and Mac OS X were not impacted.

The Department of Homeland Security has joined the chorus of impacted services urging consumers to change their passwords on updated sites. In a statement, the agency notes no attacks or incidents tied to Heartbleed have been confirmed.

"We have been and continue to work closely with federal, state, local and private sector partners to determine any potential impacts and help implement mitigation strategies as necessary," says the department in a statement.

Tech site Mashable has compiled a list of sites and services to determine whether passwords should be updated immediately.

We Need a National Change Your Passwords Day

Heartbleed, the major flaw that left passwords and other user information vulnerable to hackers this week, wasn t the first security flaw to affect the Internet. And it won t be the last. Security failures, hacks, leaks, and vulnerability discoveries are inevitable. As is the typical reaction: When news of a hack surfaces, we worry, and then some of us spring to action, generally changing passwords on affected accounts especially if the affected sites force us to.

But you should change your passwords regularly, even if you aren t facing down a flaw like Heartbleed. What we need is a National Change Your Passwords Day so you don t forget. Here s why.

One thing Heartbleed has shown us is that there are hacks and attacks, which sometimes we hear about and react to, and then there are the more worrisome discoveries of security flaws, which are worse.

Heartbleed was a discovery, not an attack. A team of security engineers

discovered a flaw in a version of common software, OpenSSL, that many major sites (and many more minor ones) use to protect and encrypt users data. This flaw had existed for over two years; it was only now discovered.

The discovery of this flaw doesn t necessarily mean that bad guys have been exploiting it, and it doesn t point to any specific attacks. Rather, it means that if anyone else (like, say,the NSA) also discovered this bug between the time when it was first included in the software, and when the Heartbleed discovery team told the world about it, they could have been using it to access or attack your data.

There is no way to completely protect yourself from threats you don t know about. But you can and should take precautions. The most obvious precaution: Limiting your exposure to individual hacks by making sure you have a unique and strong password for each different online account. I can t stress enough how important it is to have different passwords for different accounts. It s more important than having strong (unguessable) passwords, in fact. The only reasonable way to manage all these different passwords is with a password manager. I wrote a primer on these apps back in February.

Now, you can t know when a flaw like Heartbleed exists until someone discovers it, and having a unique and strong password on an account doesn t mean that another flaw isn t leaving you exposed anyway, even if you re doing all the right things. So one more thing you can do is change your passwords regularly.

Since changing a lot of passwords is a colossal pain the neck (and I mean massively inconvenient), even with a good password manager to help you, perhaps it d be best if you set aside a big chunk of time to do it. Like, a day. Maybe, in fact, a day off from work. A paid day off from work. Hey, I can dream. And keeping people (more) secure will actually save the country money, at least compared to the potential economic catastrophe of a real, pervasive, and exploited breakdown in Internet security.

Another thing you might want to do is enable two-factor authentication (also called two-step authentication) on sites that support it, like Google and Dropbox. Two-factor authentication makes it much more difficult to sign on to an account unless you have the account owner s smartphone with you, on which a second, always-changing password (the second factor or step) is displayed. We ll have more on two-factor authentication in a future article.

So when is this new National Change Your Passwords Day? I d propose we use the transition from Standard to Daylight time as the day for this, since more clocks are setting themselves these days and we have all that extra time to mind our technology. In fact, we should do password resets more than once a year, so let s make it a twice-yearly holiday and use the transition from Daylight to Standard, too.

So here s the bad news: Even regularly changing your passwords won t completely protect you from unknown theft of your personal data. It protects you a bit more, but not completely. It can take just microseconds for a hacker s system to exploit a security flaw on a service you use. But the more often you change your locks, the less likely a stolen key will to work in them.

If you ve been hacked, and then you change your password, you re protecting yourself against future intrusion into your account. That s very good and

necessary. But the digital goods you want to protect may already have been stolen. In particular, your credit card numbers are vulnerable, if you save those numbers in online accounts.

You think it s inconvenient to change passwords? Try changing credit card numbers. You can t just call your issuers and ask for new cards just to be safe. You can report your card stolen, in which case they ll immediately deactivate your existing card send you a new one. That might take a few days, and of course any automatic payments set up on that card will fail the next time they come due.

And let s not talk about trying to change other financially-relevant data, like a social security number. (Although if an online or commerce site other than a financial institution asks for a social security number, you would be wise to wonder why.)

The good news when it comes to Heartbleed (yes, there is some), is that, as far as we know, no actual banks or brokerages used the OpenSSL software that Heartbleed attacked.

Once more, with feeling: A password manager can improve your online security while also removing a lot of the hassle of keeping different passwords. However, password managers themselves are protected by passwords, which means they could potentially become vulnerable to a Heartbleed-like vulnerability.

The good news (again!) is that of the three password managers I recommend Lastpass, 1Password, and Dashlane none are directly vulnerable to the Heartbleed flaw.

I say, directly because Lastpass and 1Password both have some small exposure. Lastpass uses OpenSSL to transmit data, but it encrypts the data before the OpenSSL software sees it, so Lastpass claims they re not vulnerable to Heartblleed attacks.

1Password has a slight possibility of a flaw if you use its synchronizing service, 1PasswordAnywhere, with Dropbox to keep your passwords in sync across devices. If you re in that camp, there s a small chance that a possible Heartbleed vulnerability on Dropbox could allow an attacker to replace your 1Password sync file with a malicious version of your file, causing havoc across your 1Password account (while not actually stealing your passwords).

So if you are using one of these password managers, you might want to read their blog posts about Heartbleed. Here they are:
Lastpass | 1Password | Dashlane.

The main takeway: As part of the Hearbleed password panic, it s a good idea to change your most important passwords now, starting with your password manager, if you have one. And then change it again, perhaps the next time National Change Your Passwords Day rolls around and you re changing all your other critical passwords.

And if you don t have a password manager, get one now.

Minnesota Court To Hear All Target Data Breach Cases

The U.S. Judicial Panel on Multidistrict Litigation ordered that the many lawsuits that accuse Target Corp of failing to protect customers from a data breach will be consolidated in the retailer’s home state Minnesota.

The order brings together 33 lawsuits across 18 districts, and potentially many more tag-along actions, before the U.S. District Judge Paul Magnuson in Minnesota.

The centralization will eliminate duplicative discovery, prevent inconsistent pre-trial rulings, and conserve the resources of the parties and the judiciary, according to the transfer order.

Target, the third-largest U.S. retailer, faces several class-action lawsuits and action from banks that could seek reimbursement for millions of dollars in losses due to fraud and the cost of card replacements.

The case is in re: Target Corporation Customer Data Security Breach Litigation; case number 02522, U.S. District Court, Minnesota.

Appeals Court Overturns Conviction of AT&T Hacker ’Weev’

A federal appeals court rules that Andrew "Weev" Auernheimer was tried in the wrong state and overturns his conviction under the Computer Fraud and Abuse Act.

A federal appeals court on Friday vacated the conviction against hacker and Internet troll Andrew Auernheimer.

Auernheimer, a security researcher who goes by the nickname "Weev," was found guilty of hacking in 2012 for accessing a non-password protected portion of AT&T’s Web site to obtain the email addresses of more than 100,000 iPad users. Auernheimer, who was convicted under the controversial Computer Fraud and Abuse Act, was sentenced to 41 months in prison.

The US Court of Appeals for the 3rd Circuit, however, did not overturn the conviction because it had come to some new revelation about the fraud law, but instead found that Auernheimer was tried in the wrong federal court.

"Although this appeal raises a number of complex and novel issues that are of great public importance in our increasingly interconnected age, we find it necessary to reach only one that has been fundamental since our country’s founding: venue," the court wrote in an opinion.

Auernheimer was originally tried and convicted in federal court in New Jersey, which the 3rd Circuit concluded was improper since neither Auernheimer nor the AT&T servers he accessed were in New Jersey.

"Evidence at trial showed that at all times relevant to this case, [Auernheimer’s co-defendant Daniel Spitler] was in San Francisco, California and Auernheimer was in Fayetteville, Arkansas," the court wrote in its opinion. "The servers that they accessed were physically located in Dallas, Texas and Atlanta, Georgia."

As a result, the appeals court ruled that the venue did not lie in New Jersey and vacated Auernheimer’s conviction. Auernheimer is expected to be released from the Allenwood Federal Penitentiary in the coming days, reported The Verge.

"Today’s decision is important beyond Weev’s specific case," Hanni Fakhoury, a staff attorney for the Electronic Frontier Foundation and one of the attorneys on Auernheimer’s appeal, said in a statement. "The court made clear that the location of a criminal defendant remains an important constitutional limitation, even in today’s Internet age."

Auernheimer and co-defendant Spitler were arrested and charged in January 2011 after they created a script to download the records from AT&T and gave the results to Gawker. Auernheimer was convicted in November 2012 of one count of conspiracy to gain unauthorized access to computers and one count of identity theft. Spitler pleaded guilty to the charges in June 2011. Their appeal, which was filed in July 2013, argued that - in addition to New Jersey being the wrong venue for the trial - Auernheimer’s actions did not violate theft because as a result of AT&T’s lax security, the information was freely available on the Internet.

In an interview with CNET in 2010, Auernheimer admitted that the hackers had compromised the AT&T 3G iPad customer Web site and released data on 120,000 accounts but said they did so with the intention of warning AT&T and protecting consumers.

Auernheimer was convicted under the CFAA, a controversial law that was enacted to deter intrusions into NORAD but was expanded over time to criminalize terms of use violations. Federal prosecutors were using the CFAA against Aaron Swartz, who committed suicide in January 2013, for performing a bulk download of academic journal articles in violation of a terms of use agreement.

Feds Address Antitrust Concerns On Cyberthreat Sharing

The Justice Department and the Federal Trade Commission are trying to allay private-sector fears that sharing cyberthreat information could be seen as a violation of antitrust laws.

In an important signal to private enterprises, on Thursday the DOJ Antitrust Division and the FTC released a joint policy statement to "make it clear that they do not believe that antitrust is - or should be - a roadblock to legitimate cybersecurity information sharing."

Sharing technical cyberthreat information is fundamentally different from sharing competitively sensitive information, the agencies explained. The policy statement covers different types of sharing, structured and unstructured, person-to-person, automated or hybrid. Information can include incident or threat reports, threat indicators, threat signatures, and alerts.

[Easing industry’s concerns for sharing cyberthreat information may also speed adoption of White House guidelines for protecting critical infrastructure. Read more: Feds Launch Cyber Security Guidelines For US Infrastructure Providers.]

The policy statement does not change anything; sharing that does not have a negative impact on competition already is allowed under the FTC’s Competitor Collaboration Guidelines and the agencies have never considered sharing of security information a violation.

The policy statement says that sharing this type of technical information is allowed and encouraged in any industry sector. "It remains the agencies' current analysis that properly designed sharing of cybersecurity threat information is not likely to raise antitrust concerns," it said.

Increased threat-information sharing has long been seen as necessary to improving the nation's cybersecurity. Despite this, actually sharing such information has remained challenging. Government agencies with access to details about cyberthreats are often reluctant to share those details with industry because of the sensitive nature of the intelligence; and industry executives are reluctant to share with government because of concerns about liability and exposure of confidential information. Concerns about antitrust laws have stymied cooperation among companies.

This does not mean that information sharing is not happening. A number of "trust networks" have been established, and a number of industry sector Information and Sharing and Analysis Centers serve as vehicles for collaboration.

But many organizations still are cautious and, in the absence of legislation specifically enabling cooperation, the administration is promoting sharing through executive action. In a February 2013 executive order, President Obama highlighted the need for government to share information with the nation's private sector. But sharing also is needed within the private sector, and the DOJ-FTC policy statement provides clearance for that.

In a White House blog post, cybersecurity coordinator Michael Daniel wrote that, "reducing barriers to information sharing is a key element of this Administration's strategy to improve the nation's cybersecurity, and we are aggressively pursuing these efforts through both executive action and legislation."

He praised the policy statement and warned of the risk of doing nothing. "Companies should assess whether the remaining risks they perceive for engaging in legitimate information sharing are greater than those they face for failing to protect their customer data, their intellectual property, and their business operations from the growing cyberthreats to them."

"Today's announcement makes clear that when companies identify a threat, they can share information on that threat with other companies and help thwart an attacker's plans across an entire industry," Daniel said.

Facebook Adds Censorship Data to Transparency Report

Content on Facebook was censored most often in India and Turkey last year, the social network revealed.

Facebook on Friday released its second official government transparency report, and this time the social network is shining a spotlight on censorship efforts.

"We have expanded on our first report to include information not only about government requests for account information, but also about government requests to restrict or remove content from our service on the

grounds that it violates local law," the social network said in a blog post.

Between July and December 2013, Facebook removed 4,765 pieces of content in response to requests from the Indian government, the most of any country. Turkey came in second with 2,014 pieces of restricted content, most of which violated local laws prohibiting defamation or criticism of Ataturk or the Turkish state.

The revelation comes after Turkish Prime Minister Recep Tayyip Erdogan last month blocked access to Twitter after the micro-blogging service ignored court orders to remove "illegal" links.

"We do not remove content from our service entirely unless we determine that it violates our community standards," Facebook said. "We take a similar approach to government requests for account information. When we receive a request for information, we carefully assess whether we are legally required to comply."

Twitter did not censor anything in the U.S., but the U.S. lead the pack with 12,598 requests for Facebook user data, impacting more than 18,000 users or accounts. Facebook provided information in response to 81 percent of those requests. The U.K. followed with 1,906 requests, 71 percent of which were granted.

The social network said it pushes back on requests that are "overly broad, vague or do not comply with legal standards." When it is required to provide information, Facebook shares only the most basic information in most cases, including a user’s name and IP address.

Last year, the social network and other Internet giants made a public push for government surveillance reform. Facebook and firms like Google, Microsoft, and Yahoo have also been pushing the U.S. for permission to provide more information about national security-related requests they receive.

The two sides finally reached a deal in January whereby the DOJ gave firms two options for reporting national security-related data, and it appears Facebook selected the first option, which lets companies disclose the number of National Security Letters (NSLs), FISA requests for content, and FISA requests for non-content in bands of 1,000. In its latest report, Facebook said it received between 0 and 999 national security letters from the U.S. between July and December 2013.

Republicans Are Granted .gop Web Domain

The Republican Party has won approval for the .gop domain from the Internet Corporation for Assigned Names and Numbers (ICANN), a move the party hopes will consolidate its online outreach efforts and make official websites easier to find. The domain will be available in 75 days.

Democrats have not countered with their own domain extension yet.
 Republicans didn t lose in 2008 and 2012 because people had trouble finding their addresses, Democratic National Committee spokesman Michael Czin told FoxNews.com.

ICANN began approving new domains last summer, adding everything from

.horse to .xyz. Some brands have had trouble securing their names, however. Retailers Patagonia and Amazon had their applications for their eponymous domains rejected after objections from South American governments who said the names should be reserved for their geographical counterparts.

Google Glass Available April 15 in U.S. for One Day Only

Google will make a limited supply of its controversial Internet-linked Glass eyewear available for purchase in the United States beginning and ending on April 15.

Anyone in the United States with $1,500 to spend on Glass will be able to join the ranks of Explorers who have gotten to test out the devices prior to them hitting the market, the California-based Internet titan said Thursday in a post at Google+ social network.

Our Explorers are moms, artists, surgeons, rockers, and each new Explorer has brought a new perspective that is making Glass better, Google said in the post.

But every day we get requests from those of you who haven t found a way into the program yet, and we want your feedback too.

On April 15, starting at 9 a.m. Eastern, Google will commence what it billed as the biggest expansion of the Explorer program to date by letting anyone in the U.S. buy the eyewear online here, noting that there would be a limited number of units available.

Google in March said it is joining forces with the frame giant behind Ray-Ban and other high-end brands to create and sell Glass Internet-linked eyewear in the United States.

The partnership with Luxottica was portrayed as Google s biggest step yet into the emerging smart eyewear market.

Luxottica brands include Oakley, Alain Mikli, Ray-Ban, and Vogue-Eyewear.

The first smart glasses by Luxottica for Google Glass will go on sale in 2015, the head of the Italian eyewear group said Tuesday.

Google has been working to burnish the image of Glass, which has triggered concerns about privacy, because the devices are capable of capturing pictures and video.

Google recently sent out a release to debunk Glass myths including that it invades privacy, distracts wearers, and is for technology-worshipping geeks.

If someone wants to secretly record you, there are much, much better cameras out there than one you wear conspicuously on your face and that lights up every time you give a voice command or press a button, Google said.

If a company sought to design a secret spy device, they could do a better job than Glass.

During the Explorer testing phase, developers are creating apps for Google Glass, which can range from getting weather reports to sharing videos to playing games.

Google in February gave the early adopters a bit of advice: Don t be Glassholes.

It was the final suggestion in a recommended code of conduct posted online for the software developers and others taking part in the Explorer program.

Google appeared intent on avoiding the kinds of caustic run-ins that have seen some Glass wearers tossed from eateries, pubs, or other establishments due to concerns over camera capabilities built into devices.

Glass connects to the Internet using WiFi hotspots or, more typically, by being wirelessly tethered to mobile phones. Pictures or video may be shared through the Google+ social network.

Seven Safety Tips for People Sticking with Windows XP

Everybody panic! On Tuesday, April 8, Microsoft will stop supporting Windows XP. If you re still using a computer that s running this old operating system, you do have options. I covered them very recently: Still on Windows XP? Here s Some Bad Advice.

But what if none of the options work for you? What if, for a perfectly good reason (like the fact that upgrading from XP will cost you either money or time, and you have neither), you re stuck with a computer using XP? What s going to happen to you and your computer on April 9?

Nothing you ll notice, at least not right away. Windows XP will continue to work. But your risk of a security breach into your computer increases over time. Microsoft is adamant that Windows XP can no longer be considered a safe place to store your digital assets.

Even though the operating system has been repaired (patched) literally over 1,000 times, it s got an old foundation, and it can t stand up to modern security threats. Unless you want your data stolen, your home network hacked, or your computer taken over to be used as a slave to send spam, you need to get off this creaky platform. That s what Microsoft says.

But if you have to keep using an old XP machine, you can decrease your exposure in a few ways:

1. Get the last version.

Make sure you have the final version of Windows XP. Connect your computer to the Internet and let it update itself. Or find Windows Update on your computer and let it run. Make your version of XP as secure as possible, because it s not going to get any better after this.

The author digs out his old IBM laptop to give it one final update.

2. Update your antivirus software.

Microsoft will continue to support its own Security Essentials add-on app for Windows until July 2015. Make sure it s updated (it should handle this itself, or you can force it by opening the app and asking it to update). Security software is a strong line of defense, but it can t protect you from everything.

3. Make sure your browser is up to date.

Since the most common threats your machine is likely to see will probably come through websites you visit, be sure you re running a modern and up-to-date browser. All the current versions of the major browsers offer better security than that other giant Microsoft product that people still use, Internet Explorer 6. Get off that thing right now.

4. Be extra careful with email.

Do not open attachments on your XP computer: PDFs, Word files, attached programs, and so on. Even those that appear to be from people you know. The from line in an email message can be forged, and happy-looking emails from friends are great vectors for infection.

5. The same goes for Facebook.

It s fine to read updates, but you re at risk if you click on links to stories or sites that show up in your feed, even if they appear to be from people you know.

6. Be extra, extra careful with USB sticks, CDs, and DVDs.

These can carry malware. Your security software might catch it, but it might not. Best bet is to not use any kind of external media with this computer, especially USB sticks.

7. For the ultimate in safety, disconnect from the Internet.

Not a joke. And it s actually a workable idea for people who are using their XP computers for dedicated functions, like cash registers. If it doesn t need to be connected to the world, disconnect it. Do your email and web browsing on a modern device, like your smartphone or tablet, if you can.

Microsoft has a public document stating when it will stop supporting various versions of Windows. Today may be the end for XP, but its newer products have termination dates, too. If you re on Windows Vista (which hopefully you re not; it s terrible), you have until April 11, 2017. Windows 7 users will be abandoned on Jan. 14, 2020. The clock is even ticking on Windows 8.1: Microsoft is planning to end support for today s operating system on Jan. 10, 2023.

Time to Move On: You Can Trade in That Windows XP Machine

We ve already given you XP holdouts seven tips for braving this whole discontinuation of Microsoft support thing (which takes effect after Tuesday, by the way). In the event that you ve been officially scared off all together, consider this tip number eight:

Trade in your XP machine for money toward a new PC.

As reported by ZDNet, Best Buy is the latest retailer to offer a cash for old XP machines offer, and it s not bad. Though it stipulates the trade-in must be a laptop, you ll get a minimum of $100 that can be put toward any other computer, including a Mac or a Chromebook. The deal runs until April 19.

The Microsoft Store will also give you $100 for trading in your old XP relic, desktop or laptop, though this money can be put only toward a Windows computer, of course. This would include a Surface (original model), in the event that you re feeling frisky and want to try the switch to a more mobile Windows 8 device. The offer is good until June 15.

Even though a quick eBay search will show that there is a fair-sized niche market for powerful Windows XP computers with some selling for well over a few hundred bucks it s not likely that yours is capable of being a commercial server machine (sorry). So, unfortunately, the couple of trade-in options mentioned above are your only real chances to get a head start on buying a shiny new device.

So good luck, and don t worry about that lack of a Start menu with Windows 8. Word on the street is that it s coming back real soon.

Die, XP, Die! Why the Operating System from 2001 Won t Go Away

How can we miss Windows XP if it won t go away?

Microsoft is finally pushing this operating system out the airlock after years of ongoing support and constant updates. But the long-promised end of updates for XP today has yet to dislodge this 2001-vintage release from a dismayingly high number of computers.

StatCounter put its worldwide market share at 18.6 percent in March and no, Americans can t blame backwards foreigners for that, as XP s share in the U.S. is a full 15 percent. NetMarketShare, using different methods that factor in more computers that rarely go online, found XP on 27.7 percent of computers worldwide.

When Windows XP made its debut on Oct. 25, 2001, personal computing was a different game. We counted storage costs in dollars per gigabyte, not pennies. Cloud computing meant hoarding attached documents in a Hotmail or (ahem) Yahoo Mail account. The closest thing to a social network was the buddy list in AOL Instant Messenger.

But even just five years in, XP had aged poorly. Its security had been revealed to be so thoroughly broken that Microsoft had to ship the equivalent of a new version of Windows in the form of the massive Service Pack 2 download.

After another decade of security fixes, XP remains fundamentally insecure. Any one app can have the run of the whole system. It still needs work.

Remember, if your XP box gets hacked and enlisted into a botnet that spams people with viruses, your preference for a vintage OS suddenly

becomes everybody s problem.

Why has this fossilized release stuck around so long? In part, it s because when Microsoft had its big first chance to ship a compelling sequel to XP, it delivered Vista instead. And then it made the next update, Windows 7, a dicey upgrade from XP.

If you ve long since repressed those memories, take yourself back: Vista suffered from having the most visible part of its overdue security upgrades be the User Account Control are-you-sure? dialog that popped up every time you installed an app or maybe just looked at the computer the wrong way. Then Microsoft decided to crack down on unauthorized Windows installations except that its anti-piracy checks locked out law-abiding users too.

Oh, and many machines built for XP couldn t run Vista s slick new Aero Glass interface. In fact, until October 2010, Microsoft had to let manufacturers keep shipping the old XP operating system on the underpowered netbook laptops that had hit the market.

Windows 7 fixed many of those things, but Microsoft made upgrading from XP to 7 something to dread: In some scenarios, Windows 7 s installer would nuke your existing setup, leaving you to reload all your apps, settings and data from a backup.

Some businesses that had committed to Windows in general found their way blocked, too. The worst-case scenario involved companies and government agencies that had custom software written for XP. They became stuck there. In some cases, upgrading to a newer flavor of Windows would have been a function of spending millions of dollars to rewrite the software, Intel Security vice president Candace Worley said at a conference in Washington last week.

Similar migration woes plagued consumers. For example, if you used an older version of Intuit s QuickBooks software to manage a home business, going from XP to Windows 7 would mean buying a new release, even if you didn t need any of its new features. And just a few weeks ago, I had to enlist a Mac to get some footage off a neighbor s 2003 Sony camcorder, because Sony had not shipping post-XP driver software for USB video transfer.

(Meanwhile, Apple has gotten its developers to leap through so many hoops rewriting apps for PowerPC chips in the mid 90s, rewriting them again for OS X around the turn of the century, then a third time for Intel processors.)

For some users, the easiest upgrade is to just get a new computer. As ZDNet s longtime Windows blogger Ed Bott wrote in an e-mail, there s financial logic to that: For many of them the cost of an upgrade (including the technical help to complete the upgrade) would be equal to or larger than the cost of a new Windows 7 or 8 system.

But will all these long-time XP users be game to pay? I am betting not. I am also betting that in January of 2020, we ll see about as much angst when Microsoft terminates support for Windows 7.

Attention Windows 8.1 Users: Update 1 Is Not An Option

Windows 8.1 Update 1 (that is so clumsy) has been rolling out all week and reviewers are singing hosannas to the update, which focuses on making the OS more keyboard- and mouse-friendly.

The Update is designated as an "Important" security update in Windows Update, when a more appropriate term would be "mandatory." You see, Microsoft is going to require all Windows 8.1 users to have Windows 8.1 Update 1 installed for them in order to receive future updates.

In an April 7 post discussing the update, Microsoft's Premier Field Engineering blog, Microsoft leaves no room for ambiguity.

"Failure to install this (Windows 8.1) Update will prevent Windows Update from patching your system with any future updates starting with Updates released in May 2014 (get busy!)"

So much for giving people time to test it before rolling it out. But I suspect Windows 8's enterprise penetration is minimal anyway.

However, if you are still using the original Windows 8, unmodified with the 8.1 update, then you won't need to apply Update 1. Windows 8 will be supported by Microsoft until January 12, 2016, according to the Windows 8 lifecycle page. However, there is one bit of good news: you can go straight from Windows 8 to 8.1 Update 1 without having to install 8.1 first. Update 1 is a cumulative update.

Work continues on the Windows 8 line. Microsoft has said that a restored Start Menu and windowed Metro-Style apps will eventually be available in the much-maligned operating system, a mea culpa that admits the original design was flat wrong.

Adding these features is not trivial, so I expect that it will take Microsoft some time. Some people are wondering why the Start menu wasn't included in Update 1, but if you look at Start, it's woven through the entire OS. It has to track all your apps, your document history, have integrated search for the PC and know all of your PC, since it runs the Control Panel from Start.

That's a whole lot of integration and touching virtually every component of the operating system. So it will take Microsoft some time to get that installed and properly tested. It's not something they can just bolt on.

I've experimented with Update 1. While it does finally add all of the necessary features for us keyboard and mouse users, I have a stable, smooth-functioning Windows 7 machine and see no reason to disrupt it and spend days getting back to square 1. Maybe if the day comes that I have to reinstall the OS, I'll consider moving 8.1 from the test bed to the main machine, but for now, it's just too much disruption for too little gain.

But hey, at least I'm not saying it sucks.

Half-century Milestone for IBM Mainframes

The IBM mainframe is celebrating its 50th anniversary.

The first System 360 mainframe was unveiled on 7 April 1964 and its arrival marked a break with all general purpose computers that came before.

The machines made it possible to upgrade the processors but still keep using the same code and peripherals from earlier models.

Later this year the British rival to IBM’s machine, the ICL 1900, also celebrates its 50th anniversary.

Despite their age, mainframes are still in wide use now, said Barry Heptonstall, a spokesman for IBM.

"I don’t think people realise how often during the day they interact with a mainframe," he said.

Mr Heptonstall said mainframes were behind many of the big information systems that keep the modern world humming and handled such things as airline reservations, cash machine withdrawals and credit card payments.

The machines were very good at doing small-scale transactions, such as adding or taking figures away from bank balances, over and over again, he said.

"We don’t see mainframes as legacy technology," said Charlie Ewen, chief information officer at the Met Office, which has been using mainframes for 40 years.

"Mainframes have several characteristics that are enormously valuable for us," he said. They are "resilient, robust and are very cost-effective for some of the work we do", he added.

The Met Office uses its machines to slice its data sets in many different ways for different clients and keeps them running all day every day, said Mr Ewen.

"The mainframes are the production house of our IT operation and help us provide four million forecasts a day," he said.

Mr Heptonstall said the introduction of System 360 also changed the way computers were used.

"Before System 360 arrived, businesses bought a computer, wrote programs for it and then when it got too old or slow they threw it away and started again from scratch," he said.

Kevin Murrell, co-founder of the National Museum of Computing, said the name IBM adopted for its range of machines dated from an earlier, non-computer, era.

Scientific equipment such as oscilloscopes were often built around a "main frame" on which customers could choose to put extras or add-ons specific to their research needs.

In addition, he said, in the post office the "main frame" was the part of a telephone exchange where all the incoming wires were located.

"It was quite a common name," he said.

In the early days of computers, the size of a mainframe made it easy to

distinguish it from other types of computer.

"If it was big enough to walk around then it was a mainframe," he said. "If you could get it in your living room it was a mini-computer, and if you could carry it then it was a micro."

Soon after the appearance of the System 360 family, ICL produced its own rival line of mainframes that started with the 1900. A series of events is being planned to celebrate the arrival of that machine and its successors, said Mr Murrell.

The machines have a legacy seen on many modern keyboards, he said. The "escape" key was a common way to exit from a menu system on a mainframe and the "SysRq" key on some keyboards also dates from that era of monolithic computing.

"If you were using a terminal-based system, ’System Request’ let you interrupt what you were doing and run another job," he said. "But I’m not sure it’s ever had a use in Windows."

=~=~=~=